RECEIVED
CENTRAL FAX CENTER
NOV 30 2006

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re application of: Langhammer et al.

Attorney Docket No.: ALTRP062/A603

Application No.: 09/975,094

Examiner: Callahan, Paul E.

Filed: October 10, 2001

Group: 2137

Title: METHOD AND APPARATUS FOR PROTECTING DESIGNS IN SRAM-BASED PROGRAMMABLE LOGIC DEVICES

CERTIFICATE OF FACSIMILE TRANSMISSION
I hereby certify that this correspondence is being transmitted by facsimile to fax number 571-273-8300 to the U.S. Patent and Trademark Office on November 30, 2006.

Signed: _____
Agnes Spence

PRE-APPEAL BRIEF REQUEST FOR REVIEW

Mail Stop AF
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Applicant requests review of the final rejection in the above-identified application. No amendments are being filed with this request.

This request is being filed with a Notice of Appeal.

The review is requested for the reasons stated below.

Independent claims 1, 14, 15, 16, 17, 33, 38, and 46 were rejected under 35 U.S.C. 102(b) as being unpatentable over Albrecht. Independent claim 43 was also rejected using Albrecht. In the previous office action, the Examiner objected to the Information Disclosure Statement and the Oath/Declaration. The Applicant contacted the Examiner on April 10, 2006 regarding the discrepancies with the Information Disclosure Statement originally filed on October 7, 2002 and the Oath/Declaration and the matters were believed to have been addressed.

Albrecht describes a system where "an electronic signature is generated in a predetermined manner and attached to a transferable unit of write data, to facilitate authenticating the write data before allowing the write data to be written into a protected non-

volatile storage. The write data is authenticated using a collection of secured authentication functions. Additionally, the actual writing of the authenticated write data into the protected non-volatile storage is performed by a secured copy utility." (Column 1, Lines 33-41). The Applicants submitted that Albrecht does not describe any user logic, configurable device, or programmable logic device.

The independent claims 1, 14, 15, 16, 17, 33, 38, 43, and 46 all recite disabled user logic and enabling user logic. The independent claims also recite a configurable device. Dependent claims 3, 7, 11, 20, 25, 30, 35, 40, and 44 all recite a programmable logic device (PLD).

Albrecht does not describe any "disabled user logic," "enabling user logic," or "configurable device." In the previous office action, the Examiner argued that user logic is a flash memory, and disabled user logic is write disabled flash memory. The Applicants respectfully disagreed and stated in the previous office action response that flash memory is not user logic. In fact, flash memory is not even logic. Flash memory is merely a mechanism for storing data and does not support any logic mechanisms whatsoever. The Examiner responds in the present office action by arguing that a flash memory security circuit is user logic.

The Applicants respectfully disagree. The claims recite "disabled user logic" and "enabling user logic." It is respectfully submitted that the flash security circuit described in Albrecht is always enabled. The flash security circuit is never disabled user logic that is at some point enabled. "Flash security circuit 226 protects FLASH memory 224 from unauthorized write accesses, by keeping FLASH memory 224 write disabled, and generating an SMI to invoke the secured system BIOS write data authentication functions in system management memory 222 to authenticate the write data, whenever it enables FLASH memory 224 for a write access." (column 4, lines 25-30) It is contemplated that certain lines of flash memory could be locked by writing lock bits in various flash memory lines.

Consequently, Albrecht describes flash memory that can be disabled or enabled, but does not describe any user logic that is disabled or enabled. The Examiner argues that user logic could be a flash security circuit 226, but the flash security circuit 226 is not disabled or enabled as it is believed to be always enabled.

The independent claims also recite a configurable device. The Examiner also argues that Albrecht describes a configurable device. In the previous office action response, the Applicants indicated that it is not clear what the Examiner intended to be the configurable device in Albrecht. In the current office action, the Examiner merely cites column 3, lines 32-60 as teaching a "configurable device" again without specifying what feature, item, or entity in column 3, lines 32-60 is a configurable device. Consequently, Applicants can only speculate on what the Examiner believes to be the configurable device. The Examiner could have intended that the configurable device be the flash memory or BIOS. However, a flash memory or BIOS is not a configurable device. A flash memory and a BIOS are both merely memory devices.

Furthermore, dependent claims recite a programmable logic device. Albrecht does not teach any programmable logic device. The Examiner in rejecting various depending claims, acknowledges that the cited art does not teach the use of an SRAM PLD or an EEPROM PLD, but cites Michael Barr "How Programmable Logic Works" as describing the use of EEPROM and SRAM in programmable memory devices. The Applicants recognize that SRAM PLDs are well known, but use of SRAM PLDs in the context recited by the claims is believed to be novel and nonobvious.

Various dependent claims recite a PLD as the configurable device. Assuming that somehow the Examiner's assertion that a flash memory or BIOS is a configurable device, it would make no sense at all combine Barr and Albrecht and use the PLD configurable device as a flash memory or BIOS. Both a flash memory and BIOS are meant to be inexpensive mechanisms for being persistant storage mechanisms for small amounts of data. Using a PLD as a flash memory or a BIOS would be entirely counterintuitive, and neither Barr nor Albrecht suggest such a use. A PLD includes programmable logic that can significantly slow processing. It would make no sense to use a PLD as a flash memory or BIOS.

In light of the above remarks relating to independent claims and certain dependent claims, the remaining dependent claims are believed allowable for at least the reasons noted above. Applicants believe that all pending claims are allowable and respectfully request a Notice of Allowance for this application from the Examiner. Should the Examiner believe that a telephone conference would expedite the prosecution of this application, the undersigned can be reached at the telephone number set out below.

I am the attorney or agent acting under 37 CFR 1.34

Respectfully submitted,
BEYER WEAVER & THOMAS, LLP

Godfrey K. Kwan
Attorney of Record
Reg. No. 46,850

P.O. Box 70250
Oakland, CA 94612-0250
650-961-8300

EXAMPLE INDEPENDENT CLAIMS

1. (Original) A method for controlling use of configuration data comprising:
programming a configurable device using the configuration data provided by a secure device, the programmed configurable device comprising:
disabled user logic; and
a comparator;
generating a configurable device authorization code;
transmitting the configurable device authorization code to the comparator;
generating a secure device authorization code;
transmitting the secure device authorization code to the comparator;
comparing the configurable device authorization code and the secure device authorization code; and
enabling the user logic if the configurable device authorization code and the secure device authorization code are identical.

14. (Original) A method for controlling use of configuration data comprising:
programming a configurable device using the configuration data provided by a secure device, the programmed configurable device comprising:
disabled user logic;
a decryptor;
a configurable device sequence generator; and
a comparator;
generating a configurable device authorization code using the configurable device sequence generator;

transmitting the configurable device authorization code to the comparator;
generating a first sequence in a secure device sequence generator in the secure device;
encrypting the first sequence in an encryptor in the secure device to generate a second sequence;
transmitting the second sequence to the decryptor;
decrypting the second sequence to generate a third sequence;
transmitting the third sequence as a secure device authorization code to the comparator;
comparing the secure device authorization code and the configurable device authorization code; and
enabling the user logic if the configurable device authorization code and the secure device authorization code are identical.

15. (Original) A method for controlling use of configuration data comprising:
programming a configurable device using the configuration data provided by a secure device, the programmed configurable device comprising:
disabled user logic;
a configurable device authorization code generator; and
a comparator;
generating a configurable device authorization code in the configurable device authorization code generator;
transmitting the configurable device authorization code to the comparator;
generating a secure device authorization code in a secure device authorization code generator in the secure device;
transmitting the secure device verification code to the comparator;
comparing the configurable device authorization code and the secure device authorization code; and
enabling the user logic if the configurable device authorization code and the secure device authorization code are identical.